MPR 2810.1
REVISION C
EFFECTIVE DATE: October 22, 2004
EXPIRATION DATE: October 22, 2009

MARSHALL PROCEDURAL REQUIREMENTS

IS01

SECURITY OF INFORMATION TECHNOLOGY

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Revision	A	10/06/2000	This document was completely rewritten from previous baseline version. History log added with this revision; previous history contained in Directives Manager's Reference File. Added references to applicable documents.
Revision	B	6/11/2003	Updated footer; section 1.1, seventh line: Added definition for corporate network. Deleted "for small purchases"; Section 1.3, changed "Distributed Desktop System (DDS)" to IDS "Integrated Desktop Services (IDS)"; section 1.6, first line, deleted "department manager or group leader" and replaced with "employee"; changed "name space" to "address space" in definitions and document body; changed section 1.24 to read "…benefit of the less-secure operational situation…"; flowchart 3.4.1.3, changed "Risk Management Team" to "Risk Assessment Team" and throughout the document; changed "Information Services Department (ISD)" to "Office of the Chief Information Officer (CIO)" throughout the document; changed "Protective Services Office" to "Protective Services Department" throughout the document"; section 3.2.7, changed sentence to read "…contact to the NASA Competency Center for IT Security (CCITS), and other…;" added section 3.2.16; added "…per the System Development Life Cycle guidance found in NPG 2810.1"; changed 3.2.26 to read "…per DRD-STD/CD-ITSP, Information Technology Security Plan(s)"; added "or other designated person(s)…" to section 3.3.10; section 3.3.18.1, second sentence, changed to read "The EODD will provide guidance for procedures…."; deleted "through the IT security team" from section 3.4.1.7; deleted "Limited-Privileged" from table in section 3.4.3.1; changed section 3.4.4.1 to read "…ensure that system life-cycle security practices are followed, and that a security…developed and authorized, for each…."; added "approval contingent on" to section 3.4.4.10; changed 3.4.6.2 to read "CSOs will report to the Risk Assessment Team any changes…."; changed 3.4.6.3 to read "The Risk Assessment Team will maintain and provide periodically to the ITSM a complication…."; deleted "and cognizant senior organizational manager" from section 3.4.10.4; deleted 3.4.11 and renumbered paragraphs accordingly; deleted "NPG 2810.1 and in" from 3.4.13(now 3.4.12); deleted "This is also required where technically feasible for limited privileged accounts" from 3.5.9.3; changed 3.5.9.7 to read "…administrators may not install…outbound analog telephone connections, except where specifically justified…and approved by the NACB."; added "or services" to 3.5.9.8; added "or user-owned" to 3.5.9.12; added "any Government" to 3.6.3.1; changed "NASA" to "MSFC" and "PCITS" to "CCITS" in 3.6.4.2; changed 3.7.9.1, third paragraph to read "…individual, or at least three…infrastructure by the Network Engineering Team under the direction of the Office of the CIO."; added "isolated" to fourth paragraph of 3.7.9.1; 3.7.9.1, eleventh paragraph; changed "Incident Response Team" to "Network Engineering Team"; 3.7.9.2, third paragraph, changed to read "…preserve for investigation incident evidence related to an incident of…level and will notify…"; added "preserve any incident-related evidence in the system and will" to 3.7.9.3, fourth paragraph; 3.7.9.4, third paragraph, changed to read "…response received (if any) from the hostile-probe source…."; added "at the direction of the MSFC Protective Services Department" to s3.8.2; changed 4.1 to read "…ITSM for a minimum of three (3) years from the planned effectivity date"; and changed 4.2 to read "…retained in

			original form with all authorizing signatures by the certifying line manager for a minimum of six (6) years from the planned effectivity date."
Revision	C	10/22/2004	Per the NASA HQ action, 04-DA01-0387, to identify Center-specific requirements, to remove ambiguity regarding requirements and guidelines, and to rid the system of policy or procedure documents no longer required the following changes were made: Cover sheet changed "PROCEDURES AND GUIDELINES" to "PROCEDURAL REQUIREMENTS"; header changed "Procedures and Guidelines" to "Procedural Requirements"; throughout the document every instance of "NPG" was changed to "NPR" where required; throughout the document every instance of "MPG" was changed to "MPR" where required; P.4 added "l. NPR 1441.1, 'NASA Records Retention Schedules'" and "m. MPR 1440.2, 'MSFC Records Management Program'"; section 1.12 replaced "MPG 2800.1, "Agency Information Technology Services."" with "this document"; section 1.16, added "See Appendix Z"; moved sections 1.16.1 and 1.16.2 to Appendix Z; section 1.21 replaced "being an account holding user" with "biometrics"; section 1.23, deleted "will" and added "s" to maintain; section 2, second line, replaced "will be" with "are"; sections 2.1.1 and 2.1.2, replaced "will" with "shall"; section 2.2, replaced "is responsible for" with "shall" and changed "providing" to "provide"; section 2.3, replaced "is responsible for the planning, coordination, management, and oversight of" with "shall plan, coordinate, manage and oversee"; section 2.4, replaced "is responsible for the collective" with "shall collectively"; section 2.5, replaced "are responsible for ensuring" with "shall ensure"; section 2.6, replaced "is" with "shall be"; section 2.7, replaced "is responsible for ensuring that" with "shall ensure" and on the fourth line, replaced "will" with "shall"; section 2.8, replaced "is" with "shall be"; section 2.9, replaced "are" with "shall be"; section 2.10, replaced "is responsible for developing" with "shall develop"; section 2.11, replaced "is responsible for promptly informing" with "shall promptly inform"; section 2.12, replaced "is responsible for providing" with "shall provide"; section 2.13, replaced "is responsible for ensuring that" with "shall ensure"; section 2.14, replaced "is responsible for ensuring that" with "shall ensure"; section 2.15, replaced "is responsible for" with "shall", replaced "ensuring" with "ensure", replaced "providing" with "provide", third line removed "and", replaced "implementation of" with "implement", added "and (4)", removed the next section's heading "2.16 Systems Management Office (SMO)" and replaced "The SMO is responsible for ensuring" with "ensure"; renumbered section "2.17" to "2.16" and replaced "is responsible for ensuring that" with " shall ensure"; section 3, replaced all instances of "will" with "shall" except as noted; section 3, third line, deleted "will"; section 3.2.11, third line, deleted "will"; section 3.2.17 changed the last sentence "The OCIO may act as the alternate CSO and may perform all CSO procedures and actions in the absence of the CSO." to "When identified as the alternate CSO, the OCIO performs all CSO procedures and actions in the absence of the CSO."; section 3.2.18, third line deleted "will"; section 3.2.20, second line, deleted "will"; section 3.2.21, second line deleted "will"; section 3.2.25, third line deleted "may", fourth line deleted "will"; section 3.2.29, changed "SMO" to "Protective Services Department"; section 3.2.31, last sentence, changed "SMO" to "Protective Services Department"; section 3.3.18, fourth line, deleted "will"; section 3.4.1.3, second line deleted "will"; section 3.4.1.4, third line deleted "will"; section 3.4.2.3, second sentence, changed "are" to "shall be"; section 3.4.3.4, last sentence, deleted "will"; section 3.4.4.3, sixth line, deleted "if necessary"; deleted section 3.4.4.10, "All MSFC IT security plans and plan revisions will be presented to the NACB for approval contingent on acceptable minimum content per the requirements

			of NPG 2810.1."; section 3.4.5.2, at the end of section, added "See Appendix Z, sections 3.4.5.2.1 – 3.4.5.2.5."; moved sections 3.4.5.3, 3.4.5.4, 3.4.5.5,3.4.5.6, and 3.4.5.7 to Appendix Z; section 3.4.7.4, at the end of the section added "See Appendix Z, section 3.4.7.4.1 – 3.4.7.4.2."; moved sections 3.4.7.5 and 3.4.7.6 to Appendix Z; section 3.4.9.2, second line deleted "may"; section 3.4.9.3, replaced "The removal or mitigation of certain identified high-risk … or documented in the security plan as accepted." with "The line manager shall not waive the removal or mitigation of certain …accepted risk if such vulnerabilities when not resolved in a given system, pose a grave …"; section 3.4.11.6 third line deleted "will"; section 3.4.11.7, third line deleted "will"; section 3.4.13.4 fifth line deleted "will"; section 3.5.9.6 third line changed "will" to "could"; section 3.6.4.2 fourth line deleted "will"; section 3.6.6.1 third line deleted "will"; section 3.7.3 second line deleted "will"; section 3.7.8 third line deleted "will", seventh line deleted "will"; section 3.7.9.1 second paragraph, second line, deleted "will"; ninth paragraph, fifth line, deleted "will"; section 3.7.9.2, second paragraph, fourth line, deleted "will", third paragraph third line deleted "will", seventh paragraph third line deleted "will"; section 3.7.9.3, second paragraph second line deleted "will", fourth paragraph second line deleted "will"; section 3.7.9.4, second paragraph third line and seventh line deleted "will"; section 3.7.12 second line deleted "will"; section 3.7.13 second line deleted "will", section 4.1 first line replaced "will" with "shall"; section 4.2 first line replace "will" with "shall"; Added Appendix Z [AD01 changed to IS01 on cover page and in header by Directives Manager 6-20-2005.]

TABLE OF CONTENTS

PREFACE

P.1 PURPOSE

This directive is intended for use and reference by all Marshall Space Flight Center (MSFC) civil service and contractor employees who have access to MSFC Information Technology (IT) resources. It provides direction designed to ensure that safeguards for the protection of the integrity, availability, and confidentiality of IT resources, including data, information, applications, and systems, are integrated into and support the missions of NASA. It is specifically designed to assist those with assigned IT security responsibilities to adequately fulfill those responsibilities.

P.2 APPLICABILITY

This document applies to all MSFC facilities, employees, and contractors (as provided by law or contract), where appropriate, in achieving MSFC missions, programs, projects, and institutional requirements.

These requirements apply to any MSFC outsourced IT resources, whether outsourced to another NASA Center, another Government Agency, or a commercial facility.

Facilities, resources, and personnel under a contract or grant from MSFC, whether onsite or at a college, university, or research establishment, are included in the applicability of this document to the extent prescribed by the contract or grant.

P.3 AUTHORITY

MPD 2810.1, “Security of Information Technology”

P.4 APPLICABLE DOCUMENTS

a. OMB Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources”

b. NPD 2210.1, “External Release of NASA Software”

c. NASA-STD-2813, “NASA Firewall Strategy, Architecture, Standards, and Products”

d. NPD 2810.1, “Security of Information Technology”

e. Federal Information Processing Standards Publication 112, “Password Usage”

f. NPR 2810.1, “Security of Information Technology”

g. National Training Standard for Designated Approving Authority, National Telecommunications and Information System Security Instruction (NSTISSI) No. 4012.

h. MPD 2800.1, "Management of Information Technology Systems and Services at MSFC"

i. MPD 2810.2, "Cleaning Information from Computer Equipment at MSFC"

j. MPR 3410.1, "Training"

k. MPD 2190.1, "MSFC Export Control Program"

l. NPR 1441.1, "NASA Records Retention Schedules"

m. MPR 1440.2, "MSFC Records Management Program"

P.5 REFERENCES

All of the requirements of NPR 2810.1 are included by reference in this document. In the case of conflicting requirements, the provisions contained in NPR 2810.1 shall take precedence over this document.

P.6 CANCELLATION

MPG 2810.1B dated June 11, 2003

Original signed by
Robin N. Henderson for

David A. King
Director

DOCUMENT CONTENT

1. DEFINITIONS

1.1 Authorization to Process. A written authorization by the appropriate line manager, which may take the form of a Security Plan cover letter to the MSFC IT Security Manager summarizing the results of the IT resource risk analysis; any residual risk; planned, budgeted, and scheduled corrective actions; and a certification statement of risk acceptance to process information, or a cover letter or an approval sheet with the signatures of the responsible line manager and affected data owners attached to the IT system security plan. For IT systems requiring "special management attention," the Authorization to Process is signed by the MSFC Chief Information Officer (CIO).

1.2 Corporate network. A network that is not part of the MSFC address space and is registered to another corporate entity.

1.3 Enterprise Service. A service funded and maintained by the MSFC Center Operations (CO) Directorate for Centerwide applications, including institutional network infrastructure services.

1.4 General Support Systems. Interconnected sets of information resources or systems which share common functionality under the same direct management control including hardware, software, information, data, applications, communications, and personnel. Examples of General Support Systems include: the AdminSTAR system, the Integrated Desktop Services (IDS) System, and the MSFC Institutional Area Network (IAN). Each General Support Systems has a security plan developed by the responsible organization.

1.5 IT Resource. Data and information; computers, ancillary equipment, software, firmware, and similar products; facilities that house such resources; services, including support services; and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data. This includes telecommunications systems, networks systems, and human resources.

1.6 IT Security Program. A set of policies, procedures, and guidance for ensuring the security of the Center's IT resources. It encompasses IT security management, planning, implementation, and performance evaluation, and covers all IT resources, including, but not limited to, computers, networks, telecommunications systems, applications, data, and information.

1.7 Line Manager. A civil service employee who exercises administrative or operational controls, whether directly or through delegated technical civil service or contractor staff, for a system or application in their area of responsibility, who is accountable for the operation and security of the system or application, and who authorizes the system or application to process information.

1.8 Major Application. An application that requires special attention to security due to the risk

and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or the modification of the information in the application. All major applications require "special management attention" and each has a security plan developed by the responsible organization.

1.9 MSFC Address Space. The range of network addresses that are registered to Marshall Space Flight Center.

1.10 MSFC User. An MSFC-badged civil service employee or contractor employee, including off-site contractor personnel if MSFC-badged.

1.11 Network. A collection of interconnected systems sharing similar network address space.

1.12 Network Access Control Board (NACB). A forum to review requests for disposition of IT procurement, installation, change, and architectural implementation actions, according to the stipulations included in this document.

1.13 Network Infrastructure. The Centerwide institutional facility of IT network equipment and facilities that interconnect IT systems and applications, including Virtual Private Network (VPN) connections within the MSFC address space.

1.14 Off-site Contractor. An MSFC contractor, which operates its own systems and services in its own physical space, and is connected to the MSFC network via a serial data connection.

1.15 Privileged Account. An account empowered to add, modify, or delete operating system files, application software, configurations, account privileges or passwords, audit logs, or security controls.

1.16 Security Plan. The source document that describes how the security controls for particular systems function. Documentation from the risk assessment, risk reduction analysis, and management decisions is used to prepare a security plan. See Appendix Z.

1.17 Security Review. A process overseen by the NACB that results in disposition as to whether a planned change complies with MSFC policy and meets security requirements established for the affected systems and services, and therefore is approved for implementation.

1.18 Senior Organizational Manager. An individual assigned to a directorate or office management function, as shown on the MSFC organizational chart.

1.19 Service. A multi-user IT functionality established for provision or operation of one or more IT resources.

1.20 Special Management Attention. A designation for an IT system that has been (1) identified as a "major operating system" by the MSFC CIO; (2) provides Agencywide support or life support; (3) is critical to a facility or operation under the NASA Resource Protection Program; or

(4) has been designated by the MSFC Center Director or CIO as requiring "special management attention."

1.21 Strong User Authentication. Methods and tools used to ensure the non-refutable identification of a user of an IT system or service. This includes a requirement for possessing two of the three following properties: (1) “something you know” such as a password; (2) “something you have” such as a physical key; and (3) “something you are” as in biometrics.

1.22 System. A set of information resources under the same management controls that share common functionality and require the same level of security controls.

1.23 System Administrator. An individual assigned to ensure that the protective security measures of the system are functional and who maintains its security posture through hands-on operational and security work.

1.24 Trusted System. An IT system that physically resides within an MSFC or other approved space (including those systems operated by off-site contractors, or by MSFC personnel while at home or on travel), which operates through MSFC-approved connection software and is disconnected from all non-MSFC-approved systems and networks while connected to the MSFC Private Network.

1.25 Unacceptable Risk. A situation where the probability of negative impact, coupled with the cost to recover from that impact, exceeds the benefit of the less-secure operational situation as determined by a review by the MSFC NACB.

2. RESPONSIBILITIES

All MSFC employees shall be responsible in some capacity for IT security. Specific MSFC IT security responsibilities shall be addressed by identified functions and organizations to ensure an adequate level of MSFC IT resource integrity, confidentiality, and availability.

2.1 Center Director

2.1.1 The MSFC Center Director shall appoint an IT Security Manager (ITSM) to organize and manage an IT Security Program in accordance with Federal, Agency, and MSFC policies and requirements.

2.1.2 The Center Director shall appoint a Designated Approving Authority (DAA) to accredit MSFC IT systems as required for processing national security classified information.

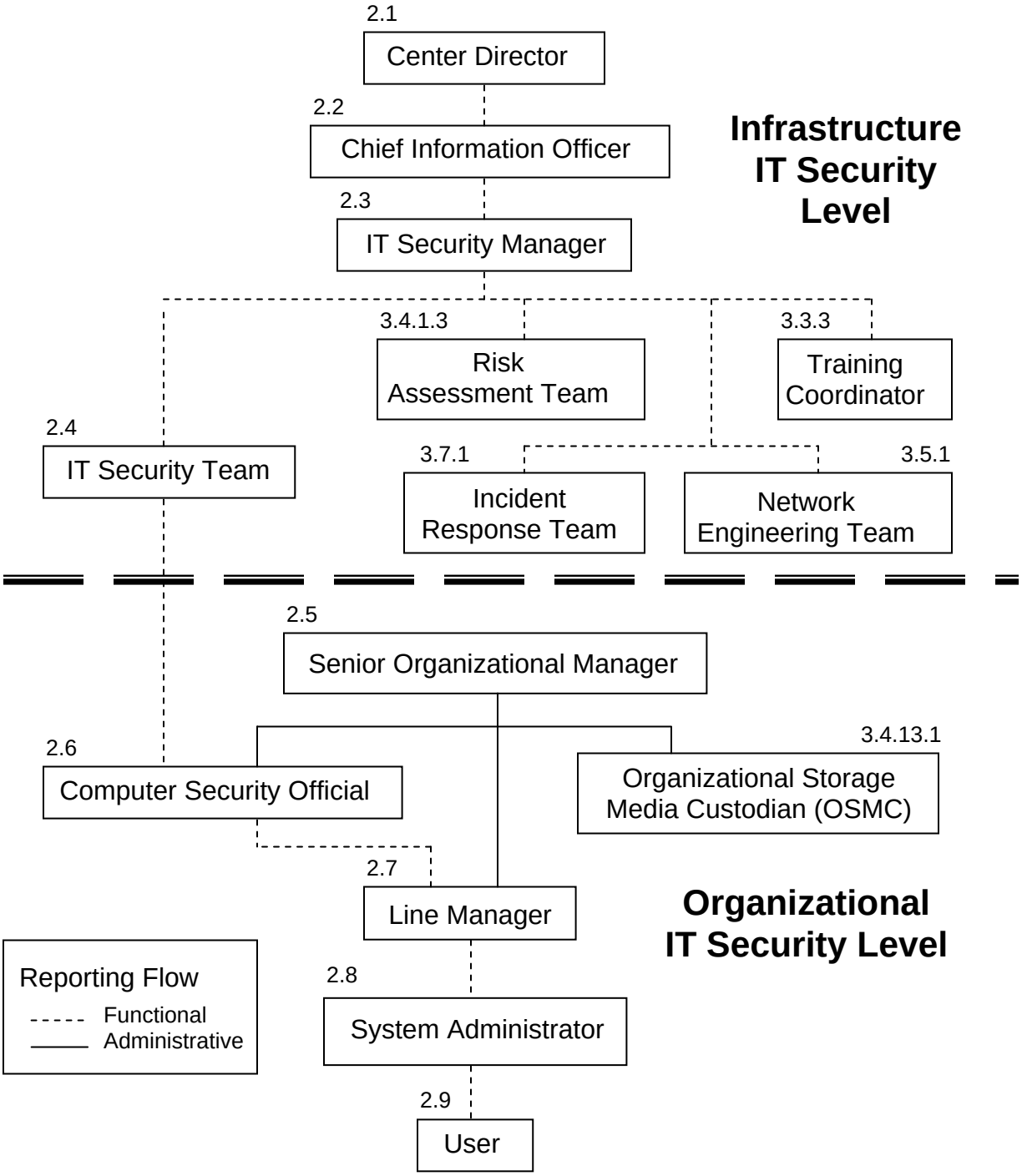


Fig. 2.1 IT Security Responsibilities Flow

2.2 Chief Information Officer (CIO)

The MSFC CIO shall provide Centerwide management oversight that ensures the security of all MSFC IT systems to adequately support the confidentiality, integrity, and availability of information processed by these systems.

2.3 IT Security Manager (ITSM)

The MSFC ITSM shall plan, coordinate, manage, and oversee initiatives and measures to ensure the confidentiality, integrity, and availability of information processed by IT systems included in the MSFC address space, consistent with the operational needs of MSFC's missions, programs, and projects.

2.4 IT Security Team

The MSFC IT Security Team shall collectively represent to the ITSM all MSFC organizations, and those contractors which are key to the security of the Center's IT assets. Duties of IT Security Team members include: (1) awareness of organizational IT security requirements and issues; (2) identification of IT systems and operational IT security environments; and (3) organizational communications concerning Centerwide IT security initiatives, actions, schedules, and events.

2.5 Senior Organizational Manager

Senior Organizational Managers shall ensure a sound IT security posture within their respective organizations, including active involvement in and support to adequate IT security planning, training, implementation, and budgeting activities.

2.6 Organizational Computer Security Official (CSO)

The organizational CSO shall be responsible for the individual organization's IT security program, the coordination of IT security initiatives and activities in the organization, and the representation of the organization at the MSFC IT Security Team for all IT security matters.

2.7 Line Manager

The line manager for a given IT system shall ensure a sound IT security posture exists for the system, including, but not limited to, security planning and risk assessment, security controls, personnel training, and incident reporting, per the minimum requirements of NPR 2810.1. If the system is operated by an MSFC contractor, this responsibility shall be assigned to the cognizant civil service manager for the contract or designated system manager.

2.8 System Administrator

The system administrator shall be responsible for the installation, configuration, operation, and maintenance of the IT system(s) within his/her area(s) of administration or control to meet the minimum requirements of NPR 2810.1.

2.9 All Employees

All MSFC civil service employees, and contractor employees to the extent of the in-force contract or grant, shall be responsible for complying with Federal, Agency, and MSFC policies, procedures, and requirements for IT security.

2.10 Employee and Organizational Development Department (EODD)

The MSFC EODD shall develop a comprehensive MSFC IT Security Training Program per requirements given in NPR 2810.1.

2.11 Human Resources Department

The Human Resources Department shall promptly inform the ITSM of personnel changes that impact the security of MSFC IT systems.

2.12 Office of the CIO

The Office of the CIO in the MSFC Center Operations Directorate shall provide (within the MSFC address space of network infrastructure) IT services that implement MSFC IT security policies, procedures, guidance and Centerwide plans to integrate the requirements and features of individual IT system security plans developed by system owner organizations.

2.13 Logistics Services Department

The Logistics Services Department shall ensure all excessed IT resources have been processed to adequately remove sensitive or inappropriate information from data storage devices contained within the resource.

2.14 Procurement Office

The Procurement Office shall ensure all MSFC contracts, grants, interagency agreements, and government orders comply with Federal, Agency, and MSFC IT security policies, procedures, and guidelines.

2.15 Protective Services Department

The Protective Services Department shall: (1) ensure the physical security of MSFC IT systems; (2) provide oversight, guidance, and approval authority for projects conducting classified activities; (3) implement a Public Key Infrastructure (PKI) at MSFC; and (4) ensure the adequate protection against inappropriate distribution of MSFC information assets which are subject to the requirements of the Export Control Program.

2.16 Technology Transfer Department (TTD)

The TTD shall ensure all MSFC external agreements properly comply with Federal, Agency, and MSFC IT security policies, procedures, and guidance.

3. PROCEDURES

System and application-level security standards shall be enforced to the greatest extent permitted by budget and contemporary technology and be implemented through the use of appropriate security procedures and guidelines.

3.1 Overview

3.1.1 All MSFC personnel and organizations are involved in some capacity in IT security implementation. The procedures to implement IT security policies at MSFC are grouped into five major areas: (1) program administration; (2) training; (3) risk management; (4) engineering; and (5) operations.

3.1.1.1 A comprehensive IT security program shall be conducted with a responsibility to manage the implementation of IT security policies and practices across all IT resources in the MSFC address space. This implementation includes individual IT system-level security responsibilities accomplished by resource owner organizations, coupled with infrastructure activities that are performed Centerwide by dedicated teams, tasked from within the IT security program itself.

3.1.1.2 IT Security Program administration shall be accomplished through the MSFC CIO, ITSM, IT Security Team, organizational CSOs, Organizational Chief Information Officers (OCIOs), and supporting functions.

3.1.1.3 An employee training program shall be provided by EODD for all MSFC civil service personnel and on-site contractor personnel, to the extent provided by the applicable contracts or grants.

3.1.1.4 Risk management processes shall be directed by the IT security program to identify, assess, and manage the threats to MSFC IT systems.

3.1.1.5 Security engineering development projects shall be planned and completed by the IT security program to provide protection to the MSFC IT asset at the network infrastructure level.

3.1.1.6 Operational procedures by the IT security program shall include computer virus protections, user authentications, national security classified information handling, and intrusion detection activities which monitor and respond to unauthorized use of MSFC IT systems.

3.1.2 All of the requirements in NPR 2810.1 are included by reference in this procedure, which clarify and extend the NPR requirements for MSFC application.

3.2 Program Administration

3.2.1 An ITSM shall provide organization and direction for implementing an MSFC IT Security Program. The ITSM shall direct and manage the MSFC IT Security Program by the coordination of the activities of the Office of the CIO, EODD, and other MSFC organizations. The ITSM shall task these MSFC organizations to deliver those products and services needed to meet minimum Federal, Agency, and Center IT security performance and schedule requirements.

3.2.2 The ITSM shall develop annual planning goals and coordinate service providers' schedules of activities to implement the IT security program.

3.2.3 The ITSM shall present periodic IT security program updates to MSFC senior management, including metrics for risk and vulnerability assessment, security plans development, intrusion and unauthorized use detection, and other program measurements.

3.2.4 The ITSM shall develop annually, with the CIO, an MSFC IT Security Plan to be submitted to the Center Director or designee for approval, per the requirements of NPR 2810.1.

3.2.5 The ITSM shall develop and maintain the MSFC IT Security Program budget from budget requirements requested and received from MSFC IT security service providers.

3.2.6 The ITSM shall establish and coordinate the activities of the IT Security Team.

3.2.7 The ITSM shall serve as the MSFC point of contact to the NASA Competency Center for IT Security (CCITS), and other Agency and Federal organizations and functions for IT security program activities and issues.

3.2.8 The CIO shall establish, maintain, and conduct policies, guidelines, and procedures necessary to ensure the IT security of MSFC IT systems has been addressed to meet the minimum requirements of applicable Federal and Agency requirements.

3.2.9 The CIO shall communicate to and from the NASA CIO concerning MSFC IT security program issues and activities.

3.2.10 The CIO shall meet regularly with the ITSM to assist in the planning and implementation of the MSFC IT Security Program goals and activities.

3.2.11 The CIO shall periodically review and revalidate MSFC IT security policies, procedures, and guidelines to ensure that they meet minimum Federal and Agency guidelines, and periodically review the architecture of MSFC networks to ensure compliance with Agency policies and requirements.

3.2.12 As a key to achieving a sound IT security posture for MSFC organizations, senior managers shall provide active support to, and involvement in, their organization's IT security activities.

3.2.13 Senior managers shall appoint an organizational CSO.

3.2.14 Senior managers shall appoint a line manager for each IT system.

3.2.15 The CSO shall develop procedures to ensure a complete, current knowledge of the organization's IT systems, security plans, operational points of contact, and overall security posture.

3.2.16 The CSO shall perform annual reviews of all security plans for IT systems in their areas per the review requirements given in the NPR 2810.1.

3.2.17 The CSO shall seek assistance if needed from MSFC organizational CIOs (OCIOs) in carrying out the organization's IT security activities. The OCIO shall represent the CIO in organizational matters. When identified as the alternate CSO, the OCIO performs all CSO procedures and actions in the absence of the CSO.

3.2.18 The CSO shall interface with the ITSM concerning the organization's IT security requirements, issues, and activities, and develop and maintain communications with the organization's IT security team representative (if different) and
OCIO in matters related to the organization's IT security posture.

3.2.19 Line managers shall identify, to the organizational CSO and the ITSM, any IT systems needing “special management attention,” as defined in NPR 2810.1.

3.2.20 For each IT system, the system line manager shall budget for and develop procedures to ensure the implementation of adequate security controls throughout the life cycle of the system, per the System Development Life Cycle requirements found in NPR 2810.1.

3.2.21 For each IT system, line managers shall appoint a system administrator and other key support staff who install, configure, operate, and maintain the system per the requirements in this MPR and NPR 2810.1.

3.2.22 An IT security team shall be chaired by the ITSM and made up of those appointed CSOs of all MSFC major organizations and on-site contractors involved in the provision of IT services.

3.2.23 The IT security team shall meet at periodic intervals as determined by the team membership. Minutes of each meeting shall be recorded and distributed to team members prior to the next meeting. Time and place of each meeting shall be announced to the membership by the ITSM prior to the meeting.

3.2.24 The IT security team shall assist the ITSM in the development of an MSFC IT Security Plan that meets the minimum requirements of NPR 2810.1.

3.2.25 IT security team representatives shall communicate among their respective organizations and the team those issues and updates which affect the IT security posture of the organization, and provide information and updates to the ITSM concerning organizational IT security system data bases, configuration requirements, and operational developments.

3.2.26 The Procurement Office shall inform the ITSM of the start of new MSFC contracts, grants, or external agreements that involve the operation of Federal IT systems. The Procurement Office shall annually provide the ITSM a summary of all existing contracts, grants and external agreements that involve the operation of Federal IT systems.

3.2.27 The Procurement Office shall include in contracts or cooperative agreements a data requirement for submission of a security plan per DRD-STD/CD-ITSP, “Information Technology Security Plan(s).”

3.2.28 The Procurement Office shall review all MSFC contracts or grants to ensure the inclusion of requirements that Government provided or funded IT systems include a warning log-on banner per the requirements of NPR 2810.1.

3.2.29 The Protective Services Department shall develop procedures to ensure that MSFC information assets are protected from inappropriate export or disclosure to non-domestic parties by means of IT resources or systems, according to the provisions of MPD 2190.1, "Export Control Program."

3.2.30 The TTD shall develop procedures to ensure that all Space Act Agreements and other external agreements which involve the development, use, or interface to MSFC IT systems meet the minimum requirements for IT security procedures by external commercial, academic, or industrial partners with the MSFC.

3.2.31 Senior managers shall implement organizational procedures to ensure that domestic and foreign release and/or distribution of computer programs developed by MSFC employees, or by non-Federal parties where intellectual property rights to the software have been assigned or licensed to the Government, are coordinated through the Center Software Releasing Authority, in

accordance with NPD 2210.1, "External Release of NASA Software," and the Protective Services Department in accordance with export control provisions contained in MPD 2190.1.

3.3 Training

3.3.1 The IT Security Program training activities shall be carried out in accordance with the provisions of MPR 3410.1, "Training."

3.3.2 The Risk Management Team Lead shall designate from within the Risk Assessment Team an IT Security Training Lead to work with the EODD.

3.3.3 The EODD shall appoint an IT Security Training Coordinator from within its organization to work with the IT Security Training Lead.

3.3.4 The EODD shall collaborate with the IT Security Training Lead to provide IT security training for MSFC personnel per requirements given in NPR 2810.1, for training at a minimum of three levels: (1) basic employee awareness; (2) management personnel responsibilities; and (3) system and network administrator duties and operations. Training schedules shall be developed by EODD and announced to MSFC personnel by the EODD.

3.3.5 The Procurement Office shall review all MSFC contracts or grants to ensure the inclusion for provision by the procuring organization of funding for adequate IT security training of contractor personnel and subcontracted workforce labor.

3.3.6 The IT Security Training Lead shall communicate to the EODD those IT security awareness and training program requirements identified by CSOs and IT security team representatives for organizational management and workforce and administrative personnel.

3.3.7 The EODD shall receive from the NASA Expert Center for IT Security Awareness and Training (ITSAT) the current definitions of required curricula for personnel performing job functions related to IT security. The IT Security Training Lead, in coordination with EODD, shall communicate this curricula information to all organizational CSOs.

3.3.8 The EODD shall develop and maintain a MSFC IT Security Awareness and Training Plan, in coordination with the IT Security Training Lead.

3.3.9 CSOs shall assist line managers and personnel supervisors in identifying the IT security training courses needed and/or completed by organizational employees to maintain job proficiency, as established by the IT security training curricula provided by the EODD IT Security Training Coordinator.

3.3.10 CSOs, or other designated person(s), shall maintain an organizational data base of employee training requirements and status for periodic reference by the IT Security Training Lead, the EODD IT Security Training Coordinator, and the ITSM, to ensure adherence to the

MSFC IT Security Awareness and Training Plan.

3.3.11 CSOs shall identify to the IT Security Training Lead those IT system administrators in their organizations who are in need of technical training and requirements for new or updated technical material to be provided at the MSFC.

3.3.12 In coordination with the IT Security Training Lead, the EODD shall allocate necessary funding to deliver training products, select appropriate training vendors, provide and schedule classroom facilities, and obtain and report participant evaluations for IT security training courses to meet the requirements of the IT security curricula established by the ITSAT, and the unique IT security training needs expressed by organizational CSOs.

3.3.13 The EODD shall provide media distribution assistance and facilities for on-line and electronic distributions of basic awareness training, manager training, and technical training courses.

3.3.14 The IT Security Training Lead shall collaborate with EODD to ensure effective distribution of IT security training course schedules and announcements within the IT security program.

3.3.15 CSOs shall identify to the IT Security Training Lead those training requirements in excess of the curricula provided by the EODD which are needed to adequately address special organizational areas.

3.3.16 Senior managers shall develop organizational procedures to ensure that IT security awareness and training provided by EODD is obtained by each employee as appropriate to their function in the organization.

3.3.17 Supervisors shall coordinate with line managers of IT systems to ensure that subordinate employees are receiving training appropriate to their assigned tasks, and that training certifications in accordance with MPR 3410.1 are updated to reflect new or changing work assignments.

3.3.18 Each employee shall obtain IT security training as required according to the employee's activity or assigned task, consisting of at least annual basic-level awareness training, and identify to the supervisor any specific additional training required to perform the job function to the minimum requirements of NPR 2810.1.

3.3.18.1 Basic Awareness Training

IT security basic awareness training shall be made available by EODD to all MSFC civil service and on-site contractor personnel by EODD, using training tools and products provided by the ITSAT through live presentations, printed media, and/or electronic distribution methods. The

EODD shall provide guidance for procedures and methods for the collection and reporting of MSFC training participation metrics to the IT Security Training Lead and the ITSAT.

3.3.18.2 Management Responsibility Training

Training products and programs as provided by the ITSAT to MSFC shall be made available by EODD for all MSFC civil service line managers, program managers, project managers, and other management personnel, concerning the security duties and responsibilities associated with the organizational ownership and security management of IT systems.

3.3.18.3 System/Network Administrator Training

Technical IT security training courses shall be obtained and made available by EODD to all MSFC civil service system/network administrator personnel as identified and required to perform their assigned job function, in order to properly fulfill the curriculum requirements established by the ITSAT.

3.4 IT Security Risk Management

3.4.1 Organizational Coordination

3.4.1.1 The MSFC CIO shall appoint a Risk Assessment Team Lead who shall select and direct a team of personnel to implement the risk management and security planning needs of the MSFC IT Security Program.

3.4.1.2 The Risk Assessment Team Lead shall serve on the standing membership of the NACB.

3.4.1.3 The Risk Assessment Team shall provide system vulnerability scanning and security audit services, and assist line managers in security planning and related risk management activities.

3.4.1.4 Line managers shall implement procedures to identify and assess security risks to each system within their area of responsibility, and take steps to mitigate the risks, through the development of a security plan per the minimum requirements of NPR 2810.1.

3.4.1.5 Line managers shall develop procedures to ensure that MSFC contractors, for their managed IT systems, enforce MSFC IT security requirements in administering accounts on their systems to the extent provided for in applicable contracts or grants.

3.4.1.6 CSOs shall periodically monitor published NASA Automated Systems Incident Response Capability (NASIRC) alerts and notices to maintain a knowledge of current threats, vulnerabilities, safeguards, toolkits, and Federal policies.

3.4.1.7 CSOs shall track the organization's implementation of NASIRC notices and alerts within

prescribed time periods, and inform the ITSM of the status of the implementation.

3.4.1.8 The Network Engineering Team shall identify upon request by a customer organization the delta costs for enhanced IT security measures to address specific risks and threats, over those provided by baseline Enterprise services, in order to meet specific program or project needs.

3.4.2 Passwords

3.4.2.1 Passwords used for user authentication to MSFC IT systems shall meet the minimum password standards as defined in NPR 2810.1.

3.4.2.2 System administrators shall implement procedures to ensure the use of non-trivial passwords per NPR 2810.1 on all administered systems.

3.4.2.3 Each user of MSFC IT systems shall develop and implement responsible password handling and usage practices as defined in NPR 2810.1. System users shall be responsible for any and all system activity generated through the use of their user IDs and passwords.

3.4.3 Personnel Access

3.4.3.1 Line managers shall grant user accesses to those systems in their areas of control, at the minimum privileges necessary for the system users to accomplish their assigned tasks. Line managers shall follow those requirements and access categories given in NPR 2810.1 to determine adequate access levels with reference to the examples below:

Information Technology Resource Access Privileges			
		Can Create/Delete/Modify	
Access Type	**User Type**	**Accounts**	**Security Controls**
Privileged	System Administrator	root, maintenance system users, system configuration	all passwords, configurations, system user ID, logs, applications
	Local Administrator	Local software installs, local users, local configuration	Local configuration, local users
	“Power” User	Local software installs, local users	Local configuration
	Maintenance Technician	Local maintenance	none
Non-Privileged	User	None	None
	Data Backup Operator	None	None

3.4.3.2 The MSFC Protective Services Department shall perform personnel background screening as requested by line managers to meet the minimum personnel access requirements in NPR 2810.1.

3.4.3.3 The Human Resources Department shall notify the ITSM of MSFC employees who have been separated from MSFC employment or who are otherwise subject to a personnel employment status change.

3.4.3.4 The MSFC Protective Services Department shall notify the ITSM of MSFC contractor personnel who have been separated from MSFC on-site employment or who are otherwise the subject of an employee status change by the contractor.

For offsite contractors/grantees with access to MSFC systems, the contracting officer in the MSFC Procurement Office shall be notified of contractor personnel status changes and report this notification to the ITSM.

3.4.3.5 The ITSM shall notify MSFC CSOs of civil service and contractor/grantee personnel with access to MSFC IT systems who have been separated from MSFC or contractor employment or otherwise subject to a personnel employment status change.

3.4.3.6 CSOs shall notify appropriate line managers and IT system administrators of those personnel access privileges to be modified or withdrawn as a result of employment separation or status changes for MSFC or contractor/grantee personnel.

3.4.3.7 The MSFC Protective Services Department shall develop and perform the necessary techniques and capabilities to act as the Center's trusted authority for supporting the identification of personnel requiring access to MSFC IT systems, and to support any subsequent assignment of user authentication procedures or facilities

3.4.4 Security Planning

3.4.4.1 Line managers shall develop procedures and practices to ensure that system life-cycle security practices are followed, and that a security plan is developed and authorized, for each IT system in their area(s) of management control before that system is put into operation to process information.

3.4.4.2 While each personal computer, workstation, or software utility need not have an individual security plan, each IT resource shall be designated as belonging to a general support system or a major IT application for which a security plan shall be developed.

3.4.4.3 IT security plans shall be based on a documented system risk assessment as described in paragraph 3.4.8, "Risk Assessment." These plans shall meet the minimum requirements of NPR 2810.1, to reflect system value, susceptibility to threat, and valid response/recovery methods. Plans shall be reviewed and updated when significant modifications are made to the system, but

in any event at least every 3 years, regardless of the system change history.

3.4.4.4 IT system security plans shall document as a minimum:
(1) the IT system function, and organizational and operational environment; (2) the system and processed information value or criticality; (3) the perceived threat to the system; (4) the in-place security controls (whether managerial, operational, technical, or developmental); (5) system configuration control and training of key personnel; (6) rationale for risk acceptance (or plans for risk mitigation); (7) plans for response and recovery from a security incident; and (8) an "authorization to process" certification by the line manager, as described in paragraph 3.4.10, "Authorization to Process."

3.4.4.5 The Risk Assessment Team shall assist the line manager with the development of security plans and updates.

3.4.4.6 The IT system administrator(s) shall ensure the IT system security plan includes a definition of all enabled software applications, operational communications ports, and communications protocols as configured in the system.

3.4.4.7 The IT system administrator(s) shall acknowledge any known security risks and all applicable operational constraints for the system, as a part of the security planning process.

3.4.4.8 CSOs shall assist with the development of IT system security plans by coordinating risk assessment and security planning team activities in the organization.

3.4.4.9 CSOs shall track the status of security plans in their organization, review with line managers the need for plan updates, and maintain file copies of the organization's plans for review by the ITSM.

3.4.5 Information Categories

3.4.5.1 All information stored, processed, or transmitted by MSFC's IT systems is sensitive to some degree and is entitled to some degree of protection. The information can be categorized into one of five designations which account for the information type, sensitivity, and criticality. For the context of this document, information categories are: (1) Mission; (2) Business and Restricted Technology; (3) Scientific, Engineering, and Research; (4) Administrative; and (5) Public Access.

3.4.5.2 All dissemination of information processed by MSFC's IT systems shall be examined by the system line manager and evaluated against the information category and content, with special emphasis given to the evaluation of information transmittal from MSFC internet web servers, in accordance with current MSFC Export Control Program and web server policies. See Appendix Z, section 3.4.5.2.

3.4.6 Inventory

3.4.6.1 The CSOs shall maintain an IT security inventory within their organization including, but not limited to: (1) owner organization, system administrator, line manager and other key contact personnel names and office hours/emergency contact information; (2) date of the most recent security risk assessment or security audit; (3) security plan approval status; (4) "authorization to process" certification status; and (5) resource equipment tracking and location information for each system in their organization.

3.4.6.2 CSOs shall report to the Risk Assessment Team any changes in their organizational IT security system inventories.

3.4.6.3 The Risk Assessment Team shall maintain and provide periodically to the ITSM a compilation of organizational IT security system inventories as provided by organizational CSOs.

3.4.7 Vulnerability Testing

3.4.7.1 The Risk Assessment Team and its delegated functions shall plan and conduct random, non-intrusive security vulnerability scans on a periodic basis for each IT resource connected to MSFC networks, and provide scan results and recommendations for the vulnerability resolution by the appropriate IT system administrator and line manager.

3.4.7.2 The Risk Assessment Team shall provide summarized reports of vulnerability scanning results to the ITSM. The ITSM shall include information summarized from Centerwide vulnerability scanning reports in periodic metrics presentations to the Center Director, and to others as required.

3.4.7.3 CSOs shall report to the ITSM those actions taken to address detected resource vulnerabilities in their organization and any inabilities to resolve the vulnerabilities.

3.4.7.4 All IT systems in the MSFC network infrastructure are subject to random scanning by the Risk Management Team, with the exception of: (1) those MSFC IT systems engaged in operational mission support during active mission timelines; and (2) critical network data handling devices. See Appendix Z, section 3.4.7.4.

3.4.7.5 IT security vulnerability testing within the MSFC address space shall be conducted only by the Risk Assessment Team, or delegated organizations, using validated commercial scanning tools. No free-ware, share-ware, or other non-validated software tools shall be utilized for vulnerability scanning purposes on any MSFC system.

3.4.7.6 Line managers shall implement procedures to ensure that vulnerabilities identified via risk assessments, security audits, or vulnerability scans are corrected according to the requirements of the IT system security plan. CSOs shall work with line managers to resolve or

mitigate identified vulnerabilities, or examine them for acceptance and documentation in the IT system security plan.

3.4.7.7 A high-risk vulnerability allows unauthorized root or administrator access to the resource. Upon repeated detection and report by the Risk Management Team of a high-risk security vulnerability on a given system, that system shall be subject to isolation from the MSFC network, following coordination with the involved organizational CSO and line manager, until such time as the vulnerability can be rectified and the system security plan updated by the line manager and approved by the NACB.

3.4.8 Risk Assessment

3.4.8.1 An IT system risk assessment process determines and documents: (1) the risks associated with a system; (2) the probability of the risk being realized; (3) the impact of a risk, if realized; (4) the priority of the risks; and (5) which risks (if any) to accept.

3.4.8.2 The line manager shall ensure that each IT system under the manager's area of management responsibility in the organization undergoes an independent risk assessment and security audit, either: (1) as a part of the security plans development or update process; or (2) following a system or information compromise of the system.

3.4.8.3 CSOs shall coordinate and schedule risk assessments of IT systems as an included part of the security plans development or update process. The risk assessment shall be conducted per the requirements in NPR 2810.1 by the Risk Assessment Team with assistance by designated key personnel for the IT system.

3.4.9 Acceptable Risk

3.4.9.1 The risk assessment process shall identify detectable IT system security risks to the extent of the tool capability and processes used in the assessment. Subsequent vulnerability scans of the IT system shall be periodically conducted to identify new or previously undetected security weaknesses.

3.4.9.2 The line manager shall work with the system administrator to remove or mitigate detected vulnerabilities, and decide to accept those weaknesses for which removal or mitigation is not technically or economically feasible. These accepted risks shall be identified in the IT system security plan.

3.4.9.3 The line manager shall not waive the removal or mitigation of certain identified high-risk vulnerabilities or document in the security plan as accepted risk if such vulnerabilities, when not resolved in a given system, pose a grave threat to the information processed by that system, or be shown to impact the security of other connected IT systems in the MSFC infrastructure.

3.4.9.4 All residual risks accepted and documented in security plans shall be reviewed and dispositioned by the NACB.

3.4.10 Authorization to Process

3.4.10.1 All MSFC IT systems shall undergo a risk assessment and security planning process with an “authorization to process” prior to the system being put into operation.

3.4.10.2 The “Authorization to Process” security plan certification by the line manager and any affected data owners for the IT system shall document that the use of the system, based on the plan, presents an acceptable level of risk to the system and the information which it processes, and that the line manager finds that the security plan as written adequately secures the IT system, its data, and its operation.

3.4.10.3 All data owners who are to process data on an IT system shall sign the security plan’s "authorization to process" as concurring on the acceptability of the system security environment to adequately protect their data.

3.4.10.4 For IT systems requiring "special management attention," the MSFC CIO shall also sign the security plan, authorizing the system to process information.

3.4.11 System Administration

3.4.11.1 System administrators shall implement procedures, controls, and checks to ensure that computer software is operated by users of the system in accordance with the vendor’s license agreement.

3.4.11.2 The ITSM shall develop procedures to distribute to CSOs those notices and alerts received from NASIRC and other information sources concerning discovered security vulnerabilities in commercial operating systems and software applications.

3.4.11.3 System administrators shall implement notices and alerts to install a software manufacturer's operating system or software application security update, whether provided through the Computer Emergency Response Team (CERT), NASIRC, or other source, according to the requirements of the IT system's security plan. System administrators shall inform the CSO of the status of the implementation of the notice, alert, or software patch.

3.4.11.4 System administrators shall install the standard NASA warning banner as described in NPR 2810.1 and referenced requirements for all administered IT systems.

3.4.11.5 System administrators shall deactivate all non-used software applications, ports, and services on all administered systems.

3.4.11.6 System administrators shall perform a check each working day of system logs and audit files to detect evidence of unauthorized use or intrusions into the system, and immediately notify the CSO and Incidence Response Team of any discovered evidence in these files of intrusions or unauthorized activity.

3.4.11.7 System administrators shall incorporate approved user identification and authentication techniques to meet the minimum requirements of NPR 2810.1, and implement advanced authentication techniques as required to maintain those security controls defined in the system security plan.

3.4.11.8 System administrators shall update user authorization and access privileges, within the time period prescribed by the ITSM, upon notification by the CSO or ITSM that a user has transferred, terminated employment, or otherwise changed employment status.

3.4.11.9 Each employee shall abide by the access and usage rules established in the security plans for those IT systems to which they have been granted access, and shall not attempt to exceed their level of granted IT access or authorization.

3.4.11.10 Each employee shall develop procedures and practices for data and information protection and data backup for the data that they "own," according to the criticality of the information, per the requirements given in NPR 2810.1.

3.4.12 Penetration Testing

Scheduled, coordinated penetration testing programs shall be conducted periodically by the MSFC Risk Assessment Team and by external testing organizations against selected MSFC IT systems with the cooperation and support of the appropriate organizational CSO, line manager, and system administrator, according to procedures included in approved penetration test documentation.

3.4.13 Information Disposal

3.4.13.1 The CSO shall recommend to the Senior Organizational Manager an employee of the organization to be appointed as the Organizational Storage Media Custodian (OSMC), to develop and implement procedures for ensuring that data storage media leaving the ownership of the organization is appropriately processed so that no data comprising NASA sensitive information or licensed software remains on the media in a manner as to be recoverable by commercially-available software tools.

3.4.13.2 The Risk Assessment Team shall specify and recommend the appropriate tools, utilities, and training for OSMCs to ensure the adequate removal from data storage media of all sensitive information and licensed software prior to excessing or ownership changes of the media.

3.4.13.3 The Logistics Services Department shall examine all MSFC IT equipment items that are being excessed to determine if the items bear documentation indicating that included data storage devices have been adequately cleared by the excessing organization of sensitive information or licensed software data.

3.4.13.4 The Logistics Services Department shall decline to process for surplus or excess action any IT equipment items that do not display documentation (labels, etc.) to clearly indicate the prior removal of sensitive information or licensed software data by the excessing organization, and notify the ITSM upon their action to decline processing.

3.5 Security Engineering

Security engineering functions shall be performed at two primary levels: (1) network-level engineering; and (2) IT system-level engineering. Infrastructure network engineering shall be performed by the Office of the CIO as MSFC's chartered institutional IT services provider. Individual IT systems-level security engineering shall be performed by appropriate system administrator and support staff as directed by the IT system line manager, within the provisions of MPD 2800.1. The NACB shall disposition requests for security engineering service or facility additions, modifications, or deletions, as originated by the Network Engineering Team for infrastructure network application, or by the appropriate line manager(s) for IT system-level issues.

3.5.1 Network Engineering Team

3.5.1.1 The Office of the CIO shall appoint an IT Security Network Engineering Team Lead who shall select and direct a team of personnel to implement the infrastructure-level network security engineering application needs of the MSFC IT Security Program.

3.5.1.2 The Network Engineering Team Lead shall participate on the standing membership of the NACB.

3.5.2 Infrastructure Network Architecture

3.5.2.1 The Network Engineering Team shall design and install an MSFC IT security infrastructure as described in NASA-STD-2813. This infrastructure shall include the following Local Area Networks (LANs): a Private Network, Public Network, Open Network, and an Agency Public Network which contains those IT services which MSFC operates for the Agency.

3.5.2.2 A Private Network shall provide maximum security safeguards for those IT systems that require protection and isolation from those IT systems and resources outside of the MSFC infrastructure. Mission-specific Private Networks are implemented within the provisions of MPD 2800.1 to address enhanced information processing needs. Corporate networks shall not be allowed within MSFC buildings as they pose a risk of interconnection to the Private Network thus compromising security safeguards.

3.5.2.3 A Public Network and Agency Public Network shall host information systems that shall be accessible by external systems while providing substantial protection including firewall services, to ensure uncompromised information integrity and service availability for these IT systems.

3.5.2.4 An Open Network shall host IT systems to provide largely unrestricted interaction with public users, without the use of firewalls.

3.5.2.5 The Private Network and the Public Network shall be separated from each other and from the global Internet by use of firewalls and/or other protective mechanisms.

3.5.2.6 The Network Engineering Team shall, at the direction of the NACB, implement and/or support per approved requirements, other program or mission-specific private networks within the MSFC network infrastructure, in accordance with the provisions of the NASA-STD 2813 to address enhanced IT security requirements.

3.5.2.7 A border router capability shall be used to further insulate the MSFC networks from those IT systems outside of the MSFC infrastructure.

3.5.3 Network Development and Configuration

3.5.3.1 The Network Engineering Team shall implement a process to ensure that network security engineering activities and initiatives do not conflict with the NASA-STD-2813, "NASA Firewall Strategy, Architecture, Standards, and Products."

3.5.3.2 The Network Engineering Team shall configure MSFC IT system interfaces to the network infrastructure to share a common host network or hardware platform, upon NACB disposition and approval, only if the systems possess similar security requirements and pose similar risks to the MSFC IT security infrastructure.

3.5.3.3 Line managers of IT systems shall request that the NACB allow off-site users to be connected to their systems within the MSFC network security hierarchy, as required and justified by mission needs.

3.5.3.4 The Network Engineering Team shall examine for network security compliance all new or developmental systems, services, or applications prior to connection to the MSFC network infrastructure.

3.5.3.5 The Network Engineering Team shall configure the connection of any given data server, service, or application to a single network only, unless directed otherwise by the NACB.

3.5.3.6 The Incident Response Team shall not reconnect to the MSFC network infrastructure any IT system which has been isolated from the network because of a security compromise until

a security audit has been completed, and the security plan updated, reviewed, and approved by the NACB for that system.

3.5.4 Open Network

3.5.4.1 In order to host services that do not initially meet the requirements of the Private Network or Public Network, an Open Network shall be provided with no security constraints to installed systems beyond those described in the Section 3.5 "Network Engineering." The Open Network shall provide no host-level security. Data availability, confidentiality, and integrity for Open Network systems shall be the responsibility of the individual system owner organization.

3.5.4.2 The Network Engineering Team shall host on the Open Network any IT system which does not meet the security requirements for either the Private Network or Public Network.

3.5.4.3 Line managers shall review with the NACB all systems hosted on the Open Network every 6 months to validate the requirement for continued Open Network hosting of the system.

3.5.4.4 The Network Engineering Team shall coordinate with contract COTRs for MSFC off-site contractors with IT systems connected to MSFC domain border routers to ensure that these off-site systems meet all requirements for the Open Network connection, with the exception of the requirement for periodic revalidation.

3.5.5 Public Network

3.5.5.1 IT systems on the MSFC Public Network are intended for use by the general public and special interest groups (e.g., scientists, educators, students, etc.), pursuant to the "National Aeronautics and Space Act of 1958," Public Law #85-568.

3.5.5.2 The Network Engineering Team shall install and maintain a firewall and/or other network protective function as approved by the NACB to control all access to IT systems hosted on the Public Network. Only those IT systems or services for which access can be controlled (i.e., proxied or filtered) by the firewall shall be hosted on the Public Network.

3.5.5.3 Upon approval by the NACB, the Network Engineering Team shall connect on the Public Network only those systems or services which require public access to accomplish MSFC's projects, programs, or missions.

3.5.5.4 The Network Engineering Team shall configure the Public Network firewall equipment to allow only inbound-originating data traffic to hosted IT systems on the Public Network. The firewall function shall block all outbound-originating network data sessions.

3.5.5.5 No developmental or test systems or services shall be hosted on the Public Network.

3.5.5.6 The Network Engineering Team shall configure the Public Network firewall or other

protective devices to allow access to privileged accounts on the Public Network by only those systems hosted by the MSFC Private Network.

3.5.5.7 IT system administrators shall configure their systems to allow access to privileged accounts only from systems hosted by the MSFC Private Network.

3.5.5.8 IT system administrators shall use off-system logging, remote system monitoring, or secure remote system administration for all IT systems and services hosted on the Public Network. Where secure remote system administration is not technically available, the system shall be administered only from a physically-attached console device until secure remote methods are available for use.

3.5.5.9 Line managers shall present for disposition by the NACB all systems and services proposed for hosting by the Public Network prior to the connection of the system or service by the Network Engineering Team onto the network.

3.5.5.10 The Network Engineering Team shall locate all Public Network systems and services on hardware platforms located within those facilities in MSFC Buildings 4207 and 4663, or other locations designated by The Office of the CIO which provide adequate access controls and environmental protections to maintain required physical security, system availability, and information integrity.

3.5.6 Agency Public Network

The Network Engineering Team shall configure those IT systems which MSFC operates for the benefit of the Agency as a whole onto the Agency Public Network. Security rules and policies for the configuration and operation of these systems are identical to those described for the MSFC Public Network.

3.5.7 Private Network

3.5.7.1 The Network Engineering Team shall propose for NACB disposition the procedures for configuration of all MSFC user workstations, including docked laptop computers and docking stations where used, to be hosted on the Private Network.

3.5.7.2 All requests for access by off-site user workstations through MSFC border router connections shall be presented for NACB review and disposition, according to the off-site user's mission/business requirements and/or contractual arrangements with MSFC.

3.5.7.3 IT system users shall, while connected to the Private Network through external accesses, secure the physical space in which the system is being used, and maintain the security of any data that is transmitted to or from the system.

3.5.7.4 Once an external connection to the Private Network is properly established through approved interfaces, all privileges and available services to the user shall be the same as if physically connected to, and within, the Private Network at MSFC.

3.5.7.5 The Network Engineering Team shall install Private Network firewalls or other protective functions per NACB directives to limit Private Network IT system access to MSFC users only, and to block all inbound-originating data traffic to the Private Network. Only those IT systems or services for which access can be controlled (i.e., proxied or filtered) by the firewall shall be hosted on the Private Network.

3.5.7.6 Line managers shall present for disposition by the NACB all systems and services proposed for hosting by the Private Network prior to the connection of the system or service by the Network Engineering Team onto the Network.

3.5.7.7 IT system administrators shall configure Private Network systems to allow access by Private Network users only.

3.5.7.8 The Network Engineering Team shall configure the MSFC network infrastructure to allow unconstrained access by Private Network systems to those systems and services external to the Private Network, including those services on the Public Network and/or Open Network, unless this access is shown to present an unacceptable risk to an MSFC IT system.

3.5.8 Network Infrastructure Protective Functions and Equipment

3.5.8.1 The Network Engineering Team shall plan, acquire, install, operate, administer, and maintain all network infrastructure firewalls and associated IT security information processing elements, as approved and directed by the NACB, to ensure the infrastructure effectiveness, compliance, and currency in the application of security rule set policies to isolate and discriminate against unauthorized network traffic onto, or through, a given network segment.

3.5.8.2 The Network Engineering Team shall functionally locate all network infrastructure protective equipment on the MSFC Institutional Area Network (IAN), or other network segments as directed by the NACB, and shall configure and maintain this equipment as an MSFC Enterprise service.

3.5.8.3 The Network Engineering Team shall specify, procure, install, and maintain all infrastructure network protective equipment to include provisions for redundancy and continuity of operations, so that any equipment failure or switching to redundant systems shall not violate the requirements of this directive.

3.5.9 System Security Engineering

Line managers for IT systems shall be responsible for ensuring the provision of a level and type of system-level security engineering which adequately protects the information processed by the

system(s) and meets the minimum requirements of the system security plan. This includes the selection and appointment of organizational system administrative staff and/or the direction of contracts to obtain individual, specialized, or otherwise unique IT security services not practically available from the Center's institutional IT service provider(s), in accordance with the provisions of MPD 2800.1.

3.5.9.1 IT system line managers shall coordinate with the organizational CSO the IT security requirements for all new, developmental, and production IT services and systems in the organization, and shall submit such requirements as requests for disposition by the NACB.

3.5.9.2 IT system administrators shall configure each IT service on a given IT system to provide a level of user access for the smallest possible audience.

3.5.9.3 IT system administrators shall use data encryption and strong user authentication using MSFC-approved technologies for privileged account access to MSFC IT systems, and is recommended for all inbound and outbound data transactions among MSFC IT systems.

3.5.9.4 IT system administrators and users shall use remote system administration, including off-system logging, remote auditing, and remote system monitoring where required.

3.5.9.5 IT system administrators shall remove or otherwise disable all unused, inactive, or unnecessary software applications, and all communications ports or sockets that are not required to enable the services provided by the system.

3.5.9.6 IT system administrators and users shall not implement data transfer protocols, practices, configurations, or other data operations which could impact the security network monitoring and intrusion detection capabilities and operations of the MSFC IT Security Incident Response Team.

3.5.9.7 IT system administrators shall only install desktop system dial-out hardware, terminal emulation software, or outbound analog telephone connections, when specifically justified by mission or business requirements and approved by the NACB.

3.5.9.8 No telephone dial-in links or services to desktop IT systems shall be permitted on any MSFC data network.

3.5.9.9 IT system administrators and users shall not use telephone modem dial-up links or any other dedicated or virtual communications links that circumvent MSFC domain firewall mechanisms.

3.5.9.10 IT system administrators or users shall not establish "back-door" data connections of IT systems to multiple network segments, or to network segments other than those designated and approved by the NACB.

3.5.9.11 IT system administrators or users shall not transmit clear-text reusable passwords across MSFC data networks, unless this practice is clearly shown to be technically unavoidable, justified in the system security plan, and approved by the ITSM.

3.5.9.12 IT system administrators and users shall not install any new or user-owned system, service, or application within the MSFC network infrastructure, or changing the configuration of an existing MSFC-networked IT system, without prior coordination with the Network Engineering Team and approval by the NACB.

3.5.10 Trust Relationships

IT system administrators and users shall establish security trust relationships between or among systems only after prior approval by the NACB. Trust relationships shall be limited to the minimum required to carry out MSFC's missions and programs.

3.5.11 Prohibited Practices

3.5.11.1 MSFC organizations other than the Risk Assessment Team, Incident Response Team, or other functionally delegated organizations, shall not use internet protocol (IP) address scanning, probing, or "sniffing" tools.

3.5.11.2 MSFC organizations shall not install or implement an IT service which, if compromised, would present a known risk of increased access or control, or decreased availability, of other IT processes, data, applications, or configurations resident on the MSFC network infrastructure. The assessment of known risk is based on relevant CERT and NASIRC warnings and current vulnerability testing results.

3.5.11.3 IT system administrators, operational and management personnel, users, and other personnel associated with an IT system shall not communicate or respond to queries regarding the configuration of MSFC IT systems or services, beyond that minimum information which is required to provide the intended and approved functionality to users as defined in the IT system security plan.

3.6 Operations

3.6.1 Physical Security

The MSFC Protective Services Department shall provide information, guidance, and assistance to IT system owners for implementation of a level of physical security which meets the minimum requirements of NPR 2810.1 for MSFC IT systems and the type of information processed by the system.

3.6.2 Viruses and Hostile Code

3.6.2.1 The Risk Assessment Team shall designate an individual to serve as the MSFC IT security alert coordinator for the direct timely dissemination of notices to MSFC IT system user personnel of evolving computer virus or hostile code attacks and recommended defenses against these situations.

3.6.2.2 The Risk Assessment Team shall coordinate the use of tools and procedures for computer virus prevention, detection, and eradication for the MSFC security network infrastructure, recommend compatible tools for use at the IT system level, and advise tool updates and changes as required to meet new identified threats by viruses and other forms of hostile code.

3.6.3 Proper Use, Privacy Notice, and Monitoring

3.6.3.1 Users of MSFC IT systems shall understand that the computer equipment, software, and contained information are the property of the U.S. Government, or other entity as specified in the contract or agreement which originally permitted access to the IT system, to be used for authorized purposes only. Unauthorized use of, or access to, any Government computer system can subject the user to disciplinary action and criminal prosecution.

3.6.3.2 Users shall recognize that they have no expectation of privacy when they use an IT system in the MSFC address space. All user activities on MSFC IT systems can be monitored to the extent provided for by current law and NASA policies. This monitoring can include traffic analysis, keystroke monitoring and recording, and examination of any or all data files on the IT system.

3.6.3.3 IT system administrators shall configure each MSFC IT system, including those operated for NASA by contractors, to display a notification and warning banner which is affirmatively displayed at the time of user log-on or at user authentication challenge to access a system, stored information, or application running on the system. Details of the proper wording and current revision for the banner can be obtained from the ITSM.

3.6.4 Data Encryption

3.6.4.1 The MSFC Protective Services Department shall develop Registration Authority (RA) and Certifying Authority (CA) procedures and operational facilities for the MSFC issuance of NASA PKI certificates to be used for, but not limited to, data encryption, digital signature, client authentication, and server authentication.

3.6.4.2 The Office of the CIO shall provide technical support to the Protective Services Department for the specification, acquisition, and installation of equipment required to implement the MSFC PKI, and serve as the technical liaison with the CCITS for design or engineering changes to the PKI.

3.6.5 Data Protection

All users and administrators of MSFC IT systems shall develop procedures and practices to protect the information processed by the system in a manner adequate to the sensitivity and value of the information. Whether performed by the user, the system administrator, or a system maintenance technician facility, the developed procedures shall implement the minimum requirements for data retention and backup as given in NPR 2810.1, Appendix A.

3.6.6 Classified Data Handling

3.6.6.1 The DAA shall ensure that sufficient measures are implemented to prevent the unauthorized recovery of encrypted data, and authorize recovery and maintain records of authorized recovery of encrypted data, as appropriate.

3.6.6.2 The MSFC Protective Services Department shall certify those IT resources involved in the processing of classified information as meeting the minimum requirements of NPR 2810.1, and the National Training Standard for Designated Approving Authority, National Telecommunications and Information System Security Instruction (NSTISSI) No. 4012.

3.7 Network Monitoring and Incident Response

3.7.1 The Office of the CIO shall appoint an Incident Response Team Lead who shall select and direct a team of individuals to implement the network monitoring and intrusion detection requirements of the MSFC IT Security Program.

3.7.2 The Incident Response Team Lead shall serve on the standing membership of the NACB.

3.7.3 The Incident Response Team shall continuously monitor data traffic on the MSFC network infrastructure and initiate response activities based on detected network intrusions and evidence of unauthorized use of MSFC IT systems.

3.7.4 The Incident Response Team shall install network traffic filters and blocks against those network addresses found to be the source of intrusions or unauthorized use of MSFC IT systems, or against discovered electronic messages bearing hostile code, or computer viruses with a potential for being received at the MSFC.

3.7.5 Each employee shall report to the cognizant IT system administrator, organizational CSO, or line manager any suspicious behavior or indications of intrusions or unauthorized use of MSFC IT resources as detected at the IT system or application level.

3.7.6 Upon detection or notification of a security incident at the IT system level, IT system administrators shall take immediate actions necessary to preserve all available evidence of the incident and to stabilize the system to limit further system or information impact.

3.7.7 System administrators shall immediately report to the Incident Response Team the detection of all IT security intrusions, unauthorized activity, or other security threats or incidents against the administrator's IT system(s). The system administrator shall also copy this information to the IT system line manager and organizational CSO.

3.7.8 System administrators shall support post-incident investigations and evidence collection processes by the Incident Response Team and perform the lead functional role in remediation of the IT system. The line manager shall support post-incident security audit activities by the Risk Assessment Team including review and revisions to the system security plan, and implement controls to ensure a reduced potential for recurrence of the incident.

3.7.9 Upon detection or notification of a network infrastructure intrusion or other security incident, the Incident Response Team shall immediately capture and retain available data traffic passing across MSFC networks as evidence of the incident, including the source and destination system network addresses and identifiers, time and date, and type of intrusion and destination response. Follow-on response activities shall be performed by the team according to the type and severity of the detected incident and different established incident categories.

3.7.9.1 System and Information Compromise Response

Upon detection or report of a system or information compromise of an IT system, the Incident Response Team shall immediately capture available incident information, including but not limited to, the time and date, relevant source and destination system network addresses and identifiers, and type of intrusion and destination response as evidence of the incident.

The Incident Response Team shall immediately begin preparation of a preliminary report of the compromise incident, and begin attempts to contact the owner organization of the IT system that is the subject of the incident.

Following positive notification of the incident to, and coordination with, the affected IT system administrator or delegated contact individual, or at least three attempted contacts with the designated individual over a 1-hour period, the compromised system shall be isolated from the MSFC data network infrastructure by the Network Engineering Team under at the direction of the Office of the CIO.

Backup copies of the operating system and data files shall be recorded by the Incident Response Team, either over the network prior to the IT system isolation, or at the system itself if already isolated, and control of the isolated IT system shall be returned to the owner organization.

In some instances of an extensive compromise or other indications of a severe intrusion, the team, at its discretion, can retain control and physical possession of the affected system for further post-compromise analysis.

A preliminary report of the incident shall be developed by the Incident Response Team within 4 hours of the incident detection and forwarded to the MSFC ITSM, the NASIRC, and to the NASA Office of Inspector General (OIG). Within 72 hours following the incident, a complete report and immediate investigation results shall be forwarded to the MSFC ITSM, the NASIRC, and the OIG.

The Incident Response Team shall inform the Risk Assessment Team of the system or information compromise.

The administrator for the compromised IT system shall inform the appropriate line manager and organizational CSO of the incident.

The IT Security Risk Management Team shall contact the line manager of the compromised system to schedule assistance for a security audit and security plan review. The IT system administrator shall rebuild and update the operating system, application, and data files software as required, and submit the affected system to a security audit by the Risk Assessment Team.

The line manager shall update the IT system security plan according to the results of the security audit by the Risk Assessment Team.

The IT system shall be reconnected to the MSFC data network infrastructure by the Network Engineering Team upon review and approval by the NACB of the updated security plan.

3.7.9.2 Unauthorized Access

An incident of unauthorized access to an IT system shall be addressed as a system compromise, with the procedures followed as given in paragraph 3.7.9.1, “System and Information Compromise Response,” until such time as the absence of information or system compromise indicators can be established by the Incident Response Team investigation.

Evidence of an unauthorized access, including, but not limited to, the time and date, source and destination system network addresses and identifiers, and type of intrusion and destination system response, shall be captured and retained by the Incident Response Team. The team shall coordinate response actions with the system administrator and notify the Risk Management Team of the incident.

The system administrator shall preserve for investigation incident evidence related to an incident of unauthorized access detected at the system or application level,, and notify the appropriate line manager and CSO of any incident of unauthorized access into administered systems.

The Risk Assessment Team shall schedule with the cognizant line manager a security audit of the affected system.

The Risk Assessment Team shall assist the line manager and system administrator in vulnerability testing of the system to address the system security weakness(es) that may have contributed to the intrusion.

The line manager shall review the system security plan for required updates according to the results of the security audit and present the updated plan to the NACB for review and disposition.

3.7.9.3 Denial of Service

A denial of service attack, in which a system function is impaired due to its being inundated with activity originating from one or more sources, shall be reported upon detection by the system administrator to the Incident Response Team.

The Incident Response Team shall assist the system administrator in capturing evidence of the incident and recommend available defenses against further attack.

The system administrator shall perform required operating system, application, and/or data file rebuilds and updates as needed to restore the system to its intended function and capability.

The system administrator shall preserve any incident-related evidence in the system and notify the appropriate line manager and CSO of the denial of service attack.

The Incident Response Team shall notify the ITSM of detected denial of service attacks against MSFC IT systems.

3.7.9.4 Hostile Probes and Scans

Upon detection of a hostile probe or scan of MSFC IT systems by an unauthorized party, the Incident Response Team shall capture relevant network traffic and source information, format this into the standard MSFC scan/probe report format, and transmit a query to the source address requesting explanatory reasons for the scan or probe.

System administrators shall, upon detection of hostile probes or scans of their systems, capture and retain evidence of the intrusion, and provide this information immediately to the Incident Response Team with copies to the IT system line manager and organizational CSO. If the CSO is not available to forward this information, the system administrator shall contact the Incident Response Team directly with the report and copy this to the CSO. In all cases, the system administrator shall also inform the cognizant line manager of the incident.

The Incident Response Team shall copy the report of the system scan/probe to the MSFC ITSM and to the NASIRC. Follow-up action shall be dependent upon the response received (if any) from the hostile-probe source address.

3.7.10 The Risk Assessment Team shall assist IT system owner and user organizations in post-incident system remediation, including the conduct of a security audit, to include: (1) a risk assessment and vulnerability scan; and (2) assistance for development of a security plan if not already in place, or a review and appropriate update for the existing plan.

3.7.11 The CSO shall provide a monthly summary to the ITSM of all security incidents in the organization.

3.7.12 The ITSM shall provide IT security incidents information and response status to the MSFC CIO and coordinate incident response reporting to MSFC, NASA, and Federal organizations.

3.7.13 The ITSM shall provide inputs to queries by the media concerning any IT security incident or event to the MSFC Media Relations Department and refer any directly received media queries to the MSFC Media Relations Department for a coordinated MSFC response.

3.8 Investigations

3.8.1 The Incident Response Team shall assist in, and provide information to support, investigations by the NASA OIG and other law enforcement organizations of misuse of MSFC IT systems.

3.8.2 The ITSM, at the direction of the MSFC Protective Services Department, shall assist the NASA OIG and other law enforcement organizations in their investigations of allegations of misuse of MSFC IT systems.

3.8.3 The ITSM shall request technical expertise from other MSFC organizations for assistance to investigations by the NASA OIG or other law enforcement organizations.

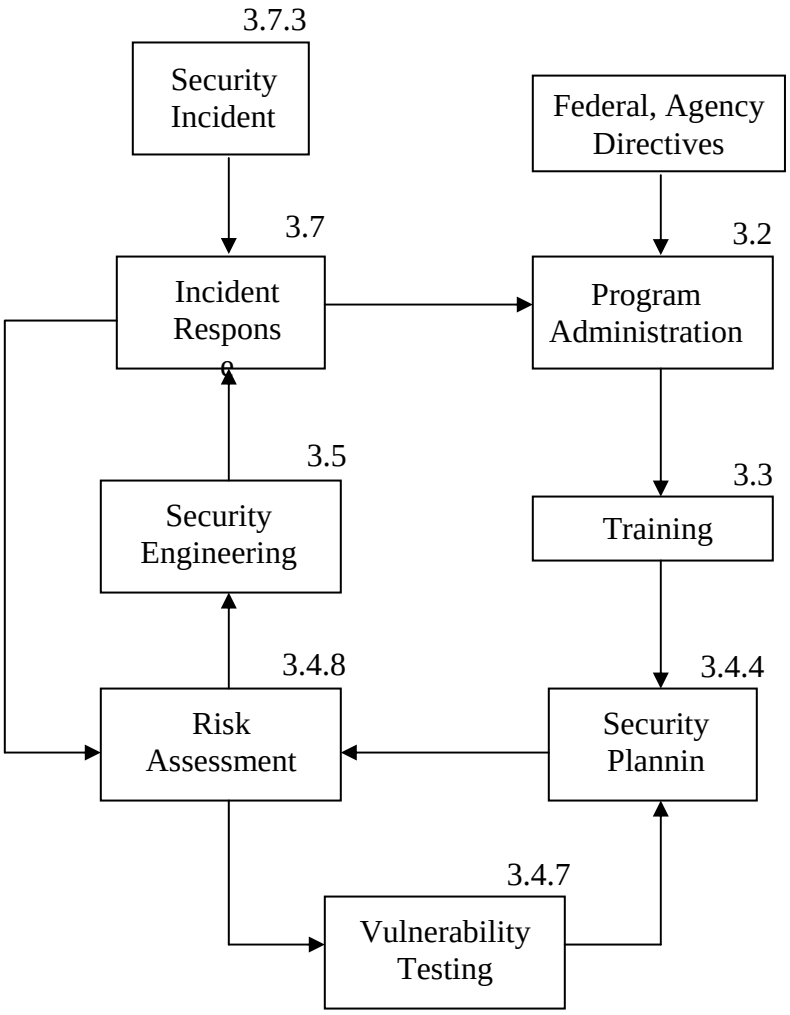
3.8.4 The MSFC Protective Services Department shall direct in the recovery or decryption of encrypted data for approved investigations into allegations of misuse of MSFC IT systems, or with any recovery of encrypted data, as approved and directed by the MSFC CIO.

4. RECORDS

4.1 Each revision of the MSFC IT Security Plan shall be retained by the ITSM for a minimum of three (3) years from the planned effectivity date.

4.2 Individual IT system security plans shall be retained in original form with all authorizing signatures by the certifying line manager for a minimum of six (6) years from the planned effectivity date.

5. FLOW DIAGRAM



Appendix Z
Guidance

1.16 Security plans for general support systems include, but are not limited to, system description, system operational rules, personnel training and controls, incident response capabilities, continuity of support, technical security capabilities, and system interfaces.

Security plans for major applications include, but are not limited to, application operational rules, specialized training, personnel security requirements, contingency planning, technical controls, information sharing constraints, and public access controls.

3.4.5.2 Mission information is that data which supports the planning and implementation of a mission, such as human space flight or launch operations. If the information were altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency mission.

Business and restricted technology information applies to systems, applications, and data which support the Agency's business and technological needs such as payroll and personnel operations. In general, if the information should be disclosed inappropriately, the disclosure could result in damage to MSFC employees, loss of business for our partners and customer businesses, contract protest, or the illegal export of technology. This category includes systems containing technological information that is restricted from general public disclosure because of public laws.

Scientific, engineering, and research information is data that supports basic research, engineering, and technology development but is less restricted against public disclosure. Alteration, destruction, unauthorized disclosure, or unavailability of the information would have an adverse or severe impact on individual projects, scientists, or engineers; however, recovery would not impede MSFC in accomplishing a primary mission.

Administrative information includes, but is not limited to, electronic correspondence, briefing information, project/program status, infrastructure design details, notes, vulnerability descriptions, passwords, and internet protocol addresses. It includes information that supports NASA’s daily activities such as electronic mail, forms processing, networking, and management reporting.

Public access information is specifically intended for public use or disclosure, such as data posted on a public web site. The loss, alteration, or unavailability of information in this category would have little direct impact on NASA’s missions but might expose the Agency to embarrassment, loss of credibility, or public ridicule.

3.4.7.4 Certain mission-critical support IT systems as defined by the NACB may be exempted from random vulnerability scanning during active mission support timelines. Scanning of these

systems during active mission timeline periods as specified by the NACB is coordinated by the Risk Assessment Team with the organizational CSO for these systems. During all other non-mission support time periods, these systems may be subject to random vulnerability scanning as are other non-exempted IT systems.

Certain critical network systems such as data routers and servers as defined by the CIO may be exempted from security vulnerabilities scanning during office hours defined as 6:00 a.m. through 6:00 p.m. local time Monday through Friday, or other periods as defined by the NACB.